Infrastructure Protection

Advanced Planning Briefing For Industry

February 21, 2006

Technical Support Working Group

Combating Terrorism Technology Support Office (CTTSO)

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for the protection and assurance of critical Government, public, and private infrastructure systems required to maintain the national and economic security of the United States.

Focus Areas:

- **Cyber Security**
- **Information Analysis**
- **Physical Protection**

Subgroup Membership

Federal Membership

DOD: OSD/HD, NSWC, NCIS, USACE, DTRA, USMC
DOJ: FBI
DOE: OEA
DHS: S&T, IA/IP, NCSD, USSS, FEMA, TSA
USDA: Forest Service
DOT: VOLPE, FAA
DOI: BOR, IFIP
OGA: NRC, EPA, BPA
Department of the Treasury

Industry Membership

Electrical Power Research Institute (EPRI)
Gas Technology Institute (GTI)

Terminology

SOTA – State of the Art

PCS – Process Control Systems

SCADA – Supervisory Control and Data Acquisition

SEI – Software Engineering Institute

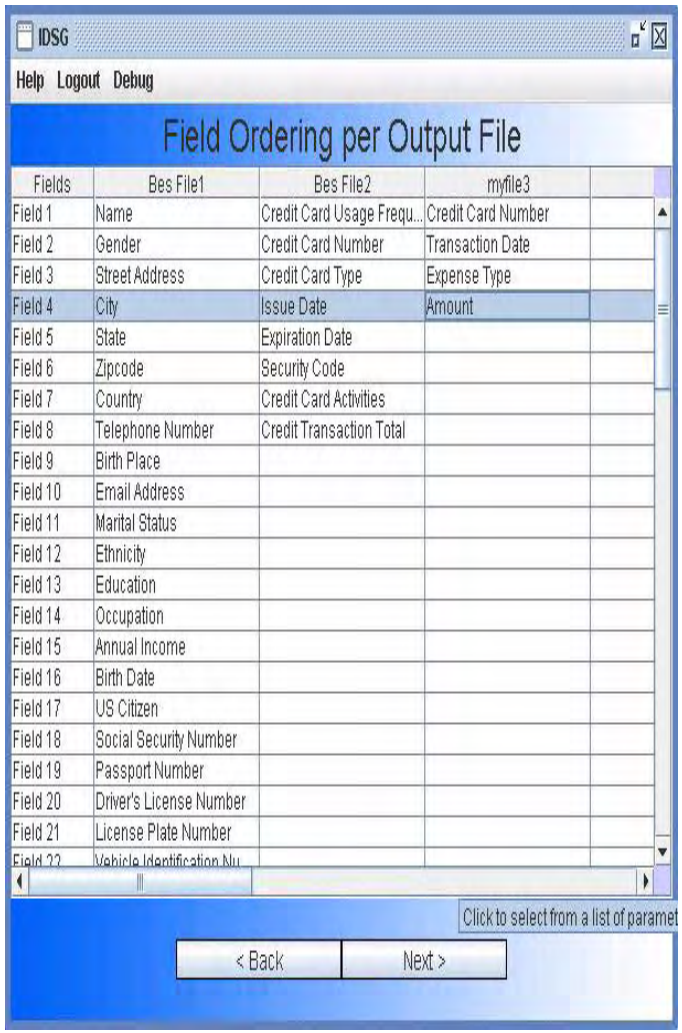
TSP – Team Software Process

O&M – Operations and Maintenance

COTS – Commercial Off The Shelf Software

GOTS – Government Off The Shelf Software

2005 Success Story



Data Set Generator (DSG)

- Lucent Technologies developed a personal data generation tool to meet FY04 BAA requirement
- Generates fictitious yet coherent datasets
- Used as a test bed for information analysis and discovery tools
- The DSG has been delivered to DHS, FBI, ARDA, and the Department of the Treasury
- For more information contact: William Sellers sellers@lucent.com

FY07 Requirements

- R2145 Secure Software Engineering Guide and Tools
- R2147 Automated Prediction, Attribution, Response and Recovery System
- R2144 Process Control Systems (PCS) Security Metrics and Testing Guide
- R2149 SCADA Cyber Attack Alert Tool
- R2148 Simulated Evacuation Planning Tool
- R2163 Transmission Tower and Line Security Monitor

R2145 Secure Software Engineering Guide and Tools

- Goal: Reduce or eliminate software vulnerabilities
- Design and develop guides and tools based on SEI TSP-Secure model
  - Best practices guidelines
  - Review methods and checklists
  - Software assessment tools that support organizational adoption
- Defined and measured best practices for individual and team developers

R2145 Secure Software Engineering Guide and Tools (cont.)

- Facilitate the implementation of TSP-Secure to assess overall software quality and to characterize defects according to their impact on:
  - Security
  - Safety
  - Reliability

- Note: Initial proof-of-concept pilot by SEI produced near defect free software with no security defects found during security audits and in several months of use

R2147 Automated Prediction, Attribution, Response & Recovery

- Automatically predict, attribute (i.e., traceback) respond and recover from network-wide cyber attacks
  - Integrate current SOTA from each area
- Identify undesirable behavior vs. predefined specific attack signatures
  - Identify behaviors of interest
  - Develop appropriate models
  - Self-learning statistical tools
  - Detect diverse spectrum of large scale attacks
  - Provide traceback and attribution of malicious cyber activity

R2147 Automated Prediction, Attribution, Response & Recovery (cont.)

- Rapid recovery and reconstitution of compromised or damaged networks by other means than traditional backups and redundancy
- Correlate information across networks or autonomous systems to provide large scale situational awareness or attack detection capability
- Demonstrate the ability to respond to zero day attacks

R2144 Process Control Systems (PCS) Security Metrics and Testing Guide

- Guide for PCS/SCADA developers, owners and operators
- Metrics for security performance based on current R&D
- PCS/SCADA Testing Methodology
- More cost-effective than general software testing approaches
- Increase the security of legacy and new PCS/SCADA

R2144 Process Control Systems (PCS) Security Metrics and Testing Guide (cont.)

- The PCS/SCADA Security Metrics and Testing Guide will consist of:
  - Security Metrics – Provides guidance on what parameters to measure
  - Testing Methodology – Provides guidance on how to make those measurements

R2149 SCADA Cyber Attack Alert Tool

- Monitor for cyber attacks that are particular to SCADA and PCS
- Alert operators to the existence, nature, and extent of cyber attacks
- Report based on a standard set of attack definitions against critical infrastructure
- Develop protocol for reporting attacks to operators and agencies
- Monitor primary and backup communications links
- Field test at a SCADA test facility to demonstrate inoperability

R2149 SCADA Cyber Attack Alert Tool (cont.)

- Aggregate and analyze reports of cyber attacks on SCADA
- Include a capability to collect data on malicious cyber activity
- Comply with existing data confidentiality, integrity, and availability standards
- Integrate with legacy systems as well as new systems
- Develop with industry cooperation and input

R2148 Simulated Evacuation Planning Tool

- Evaluate civilian evacuation responses
- Multiple types of disasters and risks
- Identify and develop strategies and risk mitigation measures
- Real-time visual simulation of crowds and vehicles
- Simulated crowds will respond to external stimuli
- Control response teams at a command level

R2148 Simulated Evacuation Planning Tool (cont.)

- Provide enough fidelity for an emergency responder simulation tool for civilian-oriented scenarios
- Import and export data formats used by other high-level simulations
- Run on a Windows laptop computer at a high resolution that allows visual assessment of results

R2163 Transmission Tower and Line Security Monitor

- Detect tampering with towers supporting electrical conductors in remote areas
- Detect structural damage or tampering on towers and lines
  - Extreme natural disasters (wind velocity, fire, and cold)
  - Unbolting the tower from its mounting points
  - Cutting the tower at its mounting and structural support points
  - Shooting insulators, and other man made acts
  - Any action that will cause the transmission line to eventually fail

R2163 Transmission Tower and Line Security Monitor (cont.)

- Communicate detection events to an operator in near real-time (<5min)
- Line voltages range from 138kV to 500kV operating at 50 or 60 Hz
- Must depend on existing infrastructure for communications and power
- No routine maintenance
- Must operate after loss of transmission line power to transmit a tampering event
- Capability for self testing and reporting of failures
- The life expectancy of the system >10 years

Contact Information

BAA Specific Questions:

06-T0032@tswg.gov